DOE CIO Guidance CS-11

U.S. Department of Energy

Cyber Security Program

MEDIA CLEARING, PURGING, AND DESTRUCTION

GUIDANCE

January 2007

This Guidance document was developed and issued outside of the Departmental Directives Program.

1. PURPOSE.

   This Department of Energy (DOE) Chief Information Officer (CIO) Guidance describes the major elements of sanitization (clearing, purging, and destruction) of electronic media, hardware, and devices. This Department of Energy (DOE) Chief Information Officer (CIO) Guidance is consistent with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-88, *Guidelines for Media Sanitization*, NIST SP 800-36, *Guide to Selecting Information Technology Security Products*, and the National Security Agency Evaluated Products List, and addresses other applicable Departmental and Federal information technology security laws and regulations.

   The DOE CIO will review this guidance annually and update it as necessary. The DOE Under Secretaries, the NNSA Administrator, the Energy Information Administration, the Power Marketing Administrations, and DOE Chief Information Officer (CIO) (hereinafter referred to as Senior DOE Management) and their subordinate organizations and contractors (hereinafter called operating units) may provide feedback at any time for incorporation into the next scheduled update.

2. SCOPE.

   This Guidance enables Senior DOE Management to address the controls in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance* and DOE Manual 205.1-4, *National Security Systems Controls Manual*, in their PCSPs. Specifically, this Guidance applies to the Media Sanitization and Media Destruction and Disposal controls in CS-1 and Clearing in DOE M 205.1-4.

   This Guidance does not negate guidance or requirements levied for specific programs or projects such as COMSEC or special programs and should be considered as minimum criteria for clearing, purging, and destruction of media.

3. CANCELLATIONS.

   None.

4. APPLICABILITY.

   a. Primary DOE Organizations. This guidance applies to all DOE Organizations listed in Attachment 1, *Primary Department of Energy Organizations to which DOE CIO Guidance CS-11 is Applicable*.

      Further, Senior DOE Management may specify and implement supplemental requirements to address specific risks, vulnerabilities, or threats within their operating units and for ensuring that those requirements are incorporated into contracts.

b. Exclusions. Consistent with the responsibilities identified in Executive Order (E.O.) 12344, the Director of the Naval Nuclear Propulsion Program will ensure consistency through the joint Navy and DOE organization of the Naval Nuclear Propulsion Program and will implement and oversee all requirements and practices pertaining to this DOE guidance for activities under the NNSA Administrator's cognizance.

c. Unclassified Systems. Senior DOE Management PCSPs must address this Guidance for all DOE systems hosting unclassified information. DOE M 471.3-1, *Manual for Identifying and Protecting Official Use Only Information*, and DOE M 471.1-1, *Identification and Protection of Unclassified Controlled Nuclear Information Manual*, provides additional information for identifying unclassified information requiring protection.

d. National Security Systems. Senior DOE Management PCSPs are to address this Guidance for all DOE National Security Systems. The protection mechanisms described in this Guidance are consistent with and implement the policies and practices set forth by Executive Order 12829 (E.O. 12829), which established the National Industrial Security Program; the requirements of the *National Industrial Security Program Operating Manual (NISPOM);* the Atomic Energy Act of 1954, which established Restricted Data information; and EO 12958, Classified National Security Information, which prescribes a uniform system for classifying, safeguarding, and declassifying national security information.. NIST SP 800-59, *Guidelines for Identifying an Information System as a National Security System*, provides additional guidance for identifying National Security systems.

5. IMPLEMENTATION.

This Guidance is effective 30 days after issuance. However, DOE recognizes that this Guidance cannot be implemented into Senior DOE Management PCSPs overnight. Except as noted below, DOE expects that Senior DOE Management shall address the criteria in this document within 90 days. If Senior DOE Management cannot address all of the criteria by this date, Senior DOE Management is to establish a Plan of Actions and Milestones (POA&M) for implementation of this Guidance into their PCSPs.

6. CRITERIA.

a. Sanitization Processes and Documentation. The Senior DOE Management PCSP must define policies, processes, and procedures for performing sanitization (clearing, purging, or destroying) of electronic media, hardware, and devices to include at least the following:

(1) Systems media and storage hardware are purged before release to personnel without authorization to access the information, including Need-to-Know, on the media or hardware.

(2) Maintenance on equipment and tools used for clearing, purging, and destruction is regularly scheduled and performed to ensure proper operation and calibration.

(3) Processes for the handling and control of media, electronic devices, and hardware prior to clearing, purging, or destruction are documented and followed.

(4) Storage media that has been used in Sensitive Unclassified Information (SUI) processing is tracked and controlled until it is purged or destroyed.

(5) The storage media must be tracked and destroyed if the confidentiality impact is moderate or high, unclassified information is located in bad sectors, or the storage media cannot be cleared or purged.

(6) Storage media that has been used in classified processing and is no longer being used or needed for archiving is tracked and controlled until it is destroyed, and the destruction is documented as required by the DOE Classified Matter Protection and Control (CMPC) program.

(7) The approval authority for sanitization procedures, software, equipment/tools, and special processes is properly identified and documented.

(8) Decision and handling processes regarding reuse of classified storage media at lower classification level(s) include formal risk and cost analyses and testing and are documented and justified.

b. Program Cyber Security Plans. Senior DOE Management PCSPs are to be consistent with the criteria in DOE OCIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*, and DOE M 205.1-4, *National Security Systems Controls Manual*. To ensure consistency with these controls, Senior DOE Management PCSPs are to direct operating units to develop, document, and implement processes for the clearing, purging, and destruction of unclassified and classified media, storage devices, and other hardware utilizing the applicable minimum criteria in Table 1, Table 2, and Table 3 and the processes described below and commensurate with the level of security required for the organization's environment and specific needs.

(1) Training and Awareness. The requirements for removing information from storage media, memory devices, and related hardware are to be reviewed with all users on a regular basis. Personnel performing or verifying the clearing, purging, or destruction of storage media, memory devices, and other hardware are to be trained in equipment/tool operation, approved techniques, and procedures.

(2) Completed purging processes are to be verified as follows:

(a) No fewer than 20 percent of the purged media are sampled on a random basis to verify the purging process has been successfully completed.

(b) The verification is conducted by individuals other than those performing the purging processes.

(c) The completion and verification of the purging process is documented.

(3) Unclassified Storage Media Processes.

(a) In addition to the processes for clearing storage media, memory, and hardware listed in Tables 1 through 3, processes to clear unclassified storage media are to include the following.

i. Storage media hosting Government information is to be cleared if it will be reused by a potential user who has a different authority for access, including Need-to-Know, or in a system that contains information whose Security Category (confidentiality, impact) is the same or higher.

ii. Only overwriting software and hardware that are compatible with media to be overwritten will be used. Care should be used to ensure a match of software and hardware to the media, considering the make, model, and manufacturing date of the media.

iii. One-pass overwrites are sufficient for clearing storage media that does not contain SUI.

iv. Individuals performing unclassified storage media clearing must certify and document successful completion of the process to include:

(i) Storage media serial number, make, and model;

(ii) The Information Type with the highest confidentiality impact hosted on the media prior to clearing;

(iii) Purpose of clearing (e.g. reuse, release, etc.);

(iv) The procedure used; and

(v) The date, the printed name, and signature of the certifier.

(b) All unclassified storage media is to be purged if the media is to be released to the public or reused on a system containing information which has a Security Category (confidentiality, impact) is less than its current use.

(c) In addition to the processes for purging storage media, memory, and hardware listed in Tables 1 through 3, processes to purge unclassified storage media are to include the following:

i. Degaussing or a minimum of three-pass overwrites is used for purging unclassified storage media that contains or did contain SUI.

ii. Individuals performing unclassified storage media purging must certify that the purging process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document:

(i) Media serial number, make, and model;

(ii) The Information Type with the highest confidentiality impact hosted on the storage media prior to purging;

(iii) Purpose of purging;

(iv) The procedure used; and

(v) The date, printed name, and signature of the certifier.

iii. Storage media that cannot be purged must be destroyed by the processes identified in Table 1.

(4) Classified Storage Media Processes.

(a) In addition to the processes for clearing storage media, memory, and hardware listed in Tables 1 through 3, processes to clear classified storage media are to include the following.

i. Storage media that will be reused on a different system for the same or more restrictive Information Group or a potential user has a different Need-to-Know must be cleared.

ii. Only overwriting software and hardware that are compatible with media to be overwritten will be used.

iii. Cleared storage media that has been used in classified processing must be protected commensurate with the highest Information Group (i.e. classification level and category of information) it has ever contained. The media must be handled in accordance with applicable DOE Classified Matter Protection and Control processes.

iv. Individuals involved in clearing classified storage media must certify and document the successful completion of the process to include:

(i) Storage media serial number, make, and model;

(ii) Most restrictive Information Group hosted prior to clearing;

(iii) Purpose for clearing;

(iv) The procedure used; and

(v) The date, the printed name, and the signature of the certifier.

(b) In addition to the processes for purging storage media, memory, and hardware listed in Tables 1 through 3 processes to purge classified storage media are to include the following.

i. Classified storage media that will be reused at a less restrictive Information Group must be purged.

ii. Classified storage media that cannot be purged must be destroyed.

iii. Classified storage media that has been purged may not be donated, sold, etc. (i.e., released from the DOE environment) to outside organizations.

iv. Individuals performing purging of classified storage media must certify the process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document:

(i) Storage media serial number, make, and model;

(ii) Most restrictive Information Group hosted prior to purging;

(iii) Purpose of purging;

(iv) A statement that the storage media contains no classified information;

(v) The procedure used; and

(vi) The date, printed name, and signature of the certifier.

v. Storage media that cannot be purged must be destroyed by the processes identified in Table 1.

(5) Special Processes. Senior DOE Management PCSPs are to direct operating units who intend to reuse classified media in an unclassified environment or decontaminate unclassified media to develop, document, and implement procedures for the processes described below.

(a) Reusing Classified Storage Media in an unclassified environment.

i. Reuse of classified storage media must be identified in the System Security Plan (SSP) of the system where the media is used and the media must be tracked/controlled until it is purged or destroyed.

ii. The storage media are to be purged by overwriting the entire storage media using the three-pass process described in Table 1.

iii. The software used is to provide information about sectors overwritten and bad sectors that cannot be overwritten.

iv. Quality controls are to be documented and deployed for review of overwrite process results and verification that all the classified information was completely overwritten

v. The storage media must be destroyed if classified information is located in bad sectors or the storage media cannot be purged.

vi. Individuals performing purging of the classified storage media planned for reuse must certify the process has been successfully completed by affixing a label to the storage media. At a minimum, the label must document:

(i) Storage media serial number, make, and model;

(ii) Most restrictive Information Group hosted prior to purging;

(iii) Purpose of purging;

(iv) A statement that the storage media contains no classified information;

(v) The procedure used; and

(vi) The date, printed name, and signature of the certifier.

(b) Purging Partially Contaminated Storage Media.

i. Areas of non-removable storage media partially contaminated with an information type of a higher confidentiality impact or more restrictive Information Group may be purged using the three-pass process described in Table 1 and continue use in its current information system in the following situations:

(i) When unclassified storage media is contaminated with relatively small amounts of classified information (less than 20 megabytes of information and less than 0.001 percent of the capacity of the non-removable storage media).

(ii) When the classified storage media is contaminated with relatively small amounts of information from a more restrictive Information Group (less than 0.1 percent of the capacity of the non-removable storage media).

(iii) When unclassified storage media operated with a confidentiality impact of low or the confidentiality impact is not applicable is

contaminated with relatively small amounts of unclassified information with a confidentiality impact of moderate or high (non-Public) (less than 0.1 percent of the capacity of the non-removable storage media).

ii. The software used to overwrite contaminated storage media must overwrite all contaminated locations, including temporary data file locations, file slack, free space, and directories; provide confirmation of overwrite of specified areas and of successful completion; and provide information about sectors overwritten and bad sectors that cannot be overwritten.

iii. Quality controls are to be documented and deployed for review of overwrite process results and verification that all the contaminating information was completely overwritten.

iv. The storage media must be destroyed if classified information is located in bad sectors or the storage media cannot be purged.

v. Records to be maintained, as a minimum, are

(i) Storage media serial number, make, and model;

(ii) Contaminating Information Group;

(iii) Purpose of purging;

(iv) A statement that the storage media no longer contains the Information Group;

(v) The procedure used; and

(vi) The date, printed name, and signature of the certifier.

TABLE 1. APPROVED PROCESSES FOR CLEARING, PURGING, AND DESTROYING STORAGE MEDIA*

MEDIA TYPE†	CLEARING‡	PURGING‡	DESTROYING‡
Magnetic Tapes			
Type I	1, 2, or 3	1, 2, 3, or 4	5
Type II	1, 2, or 3	2, 3, or 4	5
Type III	2 or 3	3 or 4	5
Magnetic Disks			
Floppies, Zip drives	1, 2, 3, or 4	X	5
Bernoulli Boxes	1, 2, 3, or 4	X	5
Removable Hard Disks	1, 2, 3, or 4	1, 2, 3, or 4	5 or 6
Non-removable Hard Disks	4	1, 2, 3, or 4	5 or 6
Optical Disks			
Magneto-optical: Read Only	X	X	5
Write Once, Read Many (WORM)	X	X	5
Read Many, Write Many	X	X	5
Other			
Floptical	X	X	5
Helical-scan Tapes	X	X	5
Cartridges	X	X	5
Optical	X	X	5
CD-R, -RW, -ROM	X	X	5 or 7
DVD	X	X	5 or 7

*NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual,* November 2000, or subsequent update may be used as a supplement for these processes when classified information is involved. NIST SP 800-88, *Guidelines for Media Sanitization*, or subsequent update may be used as a supplement for these processes when unclassified information is involved.

†DOE is responsible for developing clearing, purging, and destroying processes for media types not listed.

‡Numbers in the table refer to the processes listed.

§All degaussing products used to clear or purge media **must** be appropriate to the type of media, certified by the National Security Agency (NSA), and listed on the Degausser Products List of the NSA *Information Systems Security Products and Services Catalogue.*

Processes: †

1. Degauss with a Type 1 degausser.§
2. Degauss with a Type 2 degausser.§
3. Degauss with a Type 3 degausser.§
4. Overwrite all locations with a pseudorandom pattern twice and then with a known pattern.
5. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.

6. Remove the entire recording surfaces by sanding or applying acid.
7. Grind surface of CD or DVD to ensure the entire recording surface is removed. Only NSA Group D equipment and associated processes approved for the specific media may be used.

X. No process authorized.

TABLE 2. APPROVED PROCESSES FOR CLEARING, PURGING, AND DESTROYING ELECTRONIC MEMORY DEVICES*

MEDIA TYPE†	CLEARING†	PURGING‡	DESTROYING‡
Magnetic Bubble Memory	2	1 or 2	10
Magnetic Core Memory	2	1 or 2	10
Magnetic Plated Wire	2	2 and 3	10
Magnetic-Resistive Memory	2	X	10
Read-Only Memory (ROM)	X	X	10 (see 11)
Random Access Memory (RAM) (Volatile)	2 or 4	4, then 9	10
Programmable ROM (PROM)	X	X	10
Erasable PROM (UV PROM)	6	6, then 2 and 9	10
Electrically Alterable PROM (EAPROM)	8	7, then 2 and 9	10
Electrically Erasable PROM (EEPROM)	2	8, then 2 and 9	10
Flash Erasable PROM (FEPROM)	8	8, then 2 and 9	10

*NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual,* November 2000, or subsequent update may be used as a supplement for these processes when classified information is involved. NIST SP 800-88, *Guidelines for Media Sanitization*, or subsequent update may be used as a supplement for these processes when unclassified information is involved.

†DOE is responsible for developing clearing, purging, and destroying processes for media types not listed.

‡Numbers in the table refer to the processes listed.

§All degaussing products used to clear or purge media **must** be appropriate to the type of media, certified by the National Security Agency (NSA), and listed on the Degausser Products List of the NSA *Information Systems Security Products and Services Catalogue*.

Processes: ‡

1. Degauss with a NSA approved Type III degausser§
2. Overwrite all locations with a pseudorandom pattern twice and then with a known pattern.
3. Purging is not authorized if data resided in same location for more than 72 hours; purging is not complete until each overwrite has resided in memory for a period longer than the classified data resided in memory.
4. Remove all power, including batteries and capacitor power supplies, from RAM circuit board.
5. Perform an ultraviolet erase according to manufacturer's recommendation.
6. Perform an ultraviolet erase according to manufacturer's recommendation, but increase time requirements by a factor of 3.
7. Pulse all gates.
8. Perform a full chip purge/erase (see manufacturer's data sheet for procedure).
9. Check with CSSO to determine whether additional processes are required.
10. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure media are physically destroyed.
11. Destruction required only if ROM contained a classified algorithm or classified data.

X. No process authorized.

TABLE 3. APPROVED PROCESSES FOR CLEARING, PURGING, AND DESTROYING HARDWARE*

MEDIA TYPE†	CLEARING‡	PURGING‡	DESTROYING‡
Printer Ribbons	6	6	6
Platens	X	1	6
Toner Cartridges	5	5	X
Laser Drums	3	3	6
Cathode-Ray Tubes (If there is Classified Burn-In)	X	6	6
Fax Machines	4	4	6
Cell Phones	7	X	6
Personal Digital Assistant (PDA) (Palm, Pocket PC, etc)	7	X	6
Routers/ Copy machines	7	X	6
All other storage media devices	X	X	6

*NSA/CSS Manual 130-2, *Media Declassification and Destruction Manual*, November 2000, or subsequent update may be used as a supplement for these processes when classified information is involved. NIST SP 800-88, *Guidelines for Media Sanitization*, or subsequent update may be used as a supplement for these processes when unclassified information is involved.

†DOE is responsible for developing cleaning, purging, and destroying processes for media types not listed.

‡Numbers in the table refer to the processes listed.

Processes: †

1. Chemically clean so no visible trace of data remains.
2. Print at least five pages of randomly generated unclassified data. The pages should not include any blank spaces or solid black areas.
3. Print three blank copies. If unable to get a clean output, print an unclassified test pattern or black copy; then run three blank copies.
4. For fax machines that have memory and other storage media incorporated, treat each component per processes listed in tables 1 and 2.
5. Upon completion of copying or facsimile processing of classified material, users are required to run one or multiple blank copies to ensure the removal of all classified materials from processing device.
6. Pulverize, smelt, incinerate, disintegrate, or use other appropriate mechanisms to ensure the media is physically destroyed.
7. Manually delete all information, then perform a full manufacturers reset to reset the instrument back to factory default settings

X. Not applicable.

Note: All copies printed for clearing and purging purposes must be destroyed as classified waste.

7. REFERENCES.

   References are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls*.

8. DEFINITIONS.

   Definitions specific to this Guidance are included in Attachment 2. Acronyms and terms applicable to DOE CIO Guidance are defined in DOE CIO Guidance CS-1, *Management, Operational, and Technical Controls Guidance*.

9. CONTACT.

   Questions concerning this guidance should be addressed to the Office of the Chief Information Officer, (202) 586-0166.

ATTACHMENT 1

PRIMARY DEPARTMENT OF ENERGY ORGANIZATIONS TO WHICH GUIDANCE CS-11 IS APPLICABLE

Office of the Secretary
Office of the Chief Financial Officer
Office of the Chief Information Officer
Office of Civilian Radioactive Waste Management
Office of Congressional and Intergovernmental Affairs
Departmental Representative to the Defense Nuclear Facilities Safety Board
Office of Economic Impact and Diversity
Office of Electricity Delivery and Energy Reliability
Office of Energy Efficiency and Renewable Energy
Energy Information Administration
Office of Environment, Safety and Health
Office of Environmental Management
Office of Fossil Energy
Office of General Counsel
Office of Health, Safety, and Security
Office of Hearings and Appeals
Office of Human Capital Management
Office of the Inspector General
Office of Intelligence and Counterintelligence
Office of Legacy Management
Office of Management
National Nuclear Security Administration
Office of Nuclear Energy
Office of Policy and International Affairs
Office of Public Affairs
Office of Science
Bonneville Power Administration
Southeastern Power Administration
Southwestern Power Administration
Western Area Power Administration

ATACHMENT 2

DEFINITIONS

Clearing. Clearing information is a level of media sanitization that would protect the confidentiality of information against a robust keyboard attack. For example, overwriting is an acceptable method for clearing media.

Degaussing. Reduce the magnetic flux to virtual zero by applying a reverse magnetizing field. Also called demagnetizing.

Destroying. The result of actions taken to ensure that media cannot be reused as originally intended and that information is virtually impossible or prohibitively expensive to recover.

Disposal. Disposal is the act of discarding media with no other sanitization considerations.

Information Group. Contains all information types that require similar protection or is similar in content or use. Listed below are the Information Groups for national security or classified information.

a. Confidential/Secret (C/S) - Information that is classified Confidential National Security Information, Confidential Formerly Restricted Data, Confidential Restricted Data, Secret National Security Information, or Secret Formerly Restricted Data and does not contain any nuclear weapons data but may contain information related to uranium enrichment.

b. Secret Restricted (SR) - Information that is classified Secret Restricted Data and does not contain any nuclear weapons data but may contain information related to uranium enrichment or other Secret Restricted Data.

c. Confidential Restricted Data, Sigmas 1 through 13 (SRD1-13) - Information that is classified as Confidential and identified as Restricted Data, Formerly Restricted Data, or is related to nuclear weapons contains information that falls in at least one of the sigma categories 1 through 13 as described in DOE Order 5610.2, *Control of Weapon Data*, and successors.

d. Secret Restricted Data, Sigma 1 through 13 and 15 (SRD1-13,15) - Information that is classified as Secret and identified as Restricted Data and is related to nuclear weapons and contains information that falls within at least one of the sigma categories 1 through 13 or 15 as described in DOE Order 5610.2, *Control of Weapon Data*, and successors.

e. Secret Restricted Data, Sigma 14 and 20 (SRD14,20) - Information that is classified as Secret and identified as Restricted Data or is related to

nuclear weapons and contains information that falls within at least one of the sigma categories of 14 and 20, as described in DOE Order 5610.2, *Control of Weapon Data*, and DOE Order 457.1, *Nuclear Counterterrorism*, respectively and their successors.

f. Top Secret (TS) - Information that is classified as Top Secret National Security Information or Top Secret Formerly Restricted Data and does not contain any nuclear weapons data.

g. Top Secret Restricted Data (TSRD) - Nuclear Weapons information that is classified Top Secret.

Information Type. An information type is a specific category of information (e.g., privacy, medical, proprietary, financial, investigative, contractor sensitive, security management) defined by an organization or, in some instances, by a specific law, Executive Order, directive, policy, or regulation.

Laboratory attack. The use of a non-standard system to conduct recovery attempts on media outside their normal operating environment. This type of attack involves using signal processing equipment and highly trained personnel.

Non-removable. May not be removed without some disassembly of the information system such as case removal, removal of mounting screws or hardware, etc.

Overwrite. Writing patterns of data on top of the data stored on a magnetic medium.

Purging. Purging renders data unrecoverable by laboratory attack methods.

Sanitization. Process to remove information from media such that data recovery is not possible consisting of clear, purge, or destroy. The possibility of recovery is dependent on the environment where the sanitization occurs. It may include removing all sensitivity labels, markings, and activity logs. NIST SP 800-88, *Guidelines for Media Sanitization*, provides additional information on media sanitization methods.

Security Category. The characterization of information or an information system based on an assessment of the potential impact that a loss of confidentiality, integrity, or availability of such information or information system would have on organizational operations, organizational assets, or individuals.

Sensitive Unclassified Information (SUI) - Unclassified information requiring protection mandated by policy or laws, such as Official Use Only (OUO), Export Control Information (ECI), Unclassified Controlled Nuclear Information (UCNI), Naval Nuclear Power Information (NNPI), Personally Identifiable Information (PII), and other information specifically designated as requiring SUI protection, such information obtained under Cooperative Research and Development Agreements (CRADA).